HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10017334-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard P. Tarquini et al.

Confirmation No.: 4709

Application No.: 10/003,820

Examiner: C.G. Colin

Filing Date: October 31, 2001

Group Art Unit: 2136

Title: NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING PERFORMANCE OF SIGNATURE RULE MATCHING IN A NETWORK

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 7/26/2007.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

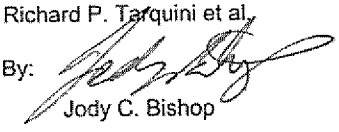
☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ _____. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,
Richard P. Tarquini et al.

By: 
Jody C. Bishop
Attorney/Agent for Applicant(s)

Reg No. : 44,034

Date : July 26, 2007

Telephone : (214) 855-8007

I hereby certify that this document is being transmitted to the Patent and Trademark Office via eletronic filing.

Date of Transmission: July 26, 2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

10017334-1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Richard P. Tarquini et al.

Application No.: 10/003,820

Confirmation No.: 4709

Filed: October 31, 2001

Art Unit: 2136

For: NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING PERFORMANCE OF SIGNATURE RULE MATCHING IN A NETWORK

Examiner: C. G. Colin

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under 37 CFR §41.37(a), this brief is filed within two months of the Notice of Appeal (which is filed concurrently herewith) and is in furtherance of said Notice of Appeal.

No further fee is believed due for this Appeal Brief because the fees required under 37 C.F.R. §41.20(b)(2) were submitted in the original Transmittal of Appeal Brief filed January 2, 2006. However, if a fee is due, please charge our Deposit Account No. 08-2025, under Order No. 10017334-1, from which the undersigned is authorized to draw.

This brief contains items under the following headings as required by 37 C.F.R. §41.37 and M.P.E.P. §1206:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Hewlett-Packard Development Company, L.P., a Limited Partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 20 claims pending in application.

B. Current Status of Claims

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-20
4. Claims allowed: none
5. Claims rejected: 1-20

C. Claims On Appeal

The claims on appeal are claims 1-20

IV. STATUS OF AMENDMENTS

A Final Office Action rejecting the claims of the present application was mailed October 24, 2006. In response, Applicant did not file an Amendment After Final Rejection, but instead filed a Notice of Appeal and supporting Appeal Brief. The Examiner did not submit an Answer, but instead reopened prosecution presenting new grounds of rejection in an Office Action mailed May 15, 2007.

In response to the May 15 Office Action, Applicant did not file an Amendment, but instead hereby files a Notice of Appeal with this supporting Appeal Brief. Accordingly, the claims on appeal are those as rejected in the Final Office Action of October 24, 2006 and again rejected in the Office Action of May 15, 2007. A complete listing of the claims is provided in the Claims Appendix hereto.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the separately argued claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. §41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. It should be noted that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

According to one claimed embodiment, such as that of independent claim 1, a node (85) of a network (100) for managing an intrusion protection system, the node (85) comprising: a memory module (274) for storing data in machine-readable format for retrieval and execution by a central processing unit (272); and an operating system (275) comprising a network stack (90) comprising a protocol driver (135) and a media access control driver (145) and operable to execute an intrusion protection system management application (279), the management application operable to receive text-file (277A-277N) input from an input device (281), the text-file (277A-277N) defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 5, the node (85) further comprises a machine-readable signature-file database (278B) operable to store a plurality of machine-readable signature-files (281A-281N) each generated from one of a respective plurality of text-files (277A-277N), the management application (279) operable to transmit a subset of the plurality of machine-readable signature-files (281A-281N) to another node (270) connected to the network (100). In certain embodiments, such as that of dependent claim 6, the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files (281A-281N) each generated from a respective text-file (277A-277N) having an asserted ENABLED field value (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 7, the management application (279) is operable to accept a SEVERITY threshold from the input device (281) and the subset comprises all machine-readable signature-files (281A-281N) respectively generated from a text-file (277A-277N) having a SEVERITY field value equal to or greater than the threshold (at least page 17, line 8 – page 21, line 2).

According to one claimed embodiment, such as that of independent claim 8, a method of distributing command and security updates in a network (100) having an intrusion protection system (91) comprising generating a text-file (277A-277N) defining a network-exploit rule, and specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file (277A-277N), *see* at least page 17, line 8 – page 21, line 2.

In certain embodiments, such as that of dependent claim 11, the subset of machine-readable signature-files (281A-281N) comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files (277A-277N) that has the respective ENABLED field asserted (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 12, the method further comprises specifying a priority level threshold, the subset of the plurality of machine-readable signature-files (281A-281N) comprised of all machine-readable signature-files generated from a respective one of the plurality of text-files (277A-277N) having a SEVERITY level field value equal to or greater than the threshold (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 19, the ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system, and wherein the SEVERITY level field value specifies a severity level of the network-exploit rule, *see e.g.,* page 18, line 14 – page 20, line 27.

In certain embodiments, such as that of dependent claim 20, the method further comprises distributing the network-exploit rule and the at least one field to a plurality of nodes;

and determining by an intrusion protection system of each of the plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node, *see* at least page 17, line 8 – page 21, line 2.

According to one claimed embodiment, such as that of independent claim 13, a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor (272), cause the processor (272) to perform a computer method of reading input from an input device (281) of the computer; compiling the input into a machine-readable signature file (281A-281N) comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field, evaluating the machine-readable signature file (281A-281N), and determining the value of the at least one field of the machine-readable signature file (281A-281N), *see* at least page 17, line 8 – page 21, line 2.

In certain embodiments, such as that of claim 15, the computer readable medium further comprises a set of instructions that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold, *see* at least page 17, line 8 – page 21, line 2.

In certain embodiments, such as that of claim 17, the computer readable medium further comprises a set of instructions that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the ENABLED field value is logically asserted, *see* at least page 17, line 8 – page 21, line 2.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-7 are rejected under 35 USC §103(a) as being unpatentable over U.S. Patent Publication No. 2002/0078381 to Farley et al. (hereinafter "*Farley*") in view of U.S. Patent No. 6,279,113 to Vaidya (hereinafter "*Vaidya*").

B. Claims 8-20 are rejected under 35 U.S.C. §102(e) as being anticipated by *Farley*.

VII. ARGUMENT

Appellant respectfully traverses the outstanding rejections of the pending claims, and requests that the Board reverse the outstanding rejections in light of the remarks contained herein. The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Rejections under 35 U.S.C. §103 over *Farley* in view of *Vaidya*

Claims 1-7 are rejected under 35 USC §103(a) as being unpatentable over *Farley* in view of *Vaidya*. Appellant respectfully traverses these rejections for at least the reasons advanced below.

The test for non-obvious subject matter is whether the differences between the subject matter and the prior art are such that the claimed subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains. The United States Supreme Court in Graham v. John Deere and Co., 383 U.S. 1 (1966) set forth the factual inquiries which must be considered in applying the statutory test: (1) determining of the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims at issue; and (3) resolving the level of ordinary skill in the pertinent art. As discussed further hereafter, Appellant respectfully asserts that the claims include non-obvious differences over the cited art.

As discussed further below, the rejections should be overturned because when considering the scope and content of the applied *Farley* and *Vaidya* references there are significant differences between the applied combination and claims 1-7, as the applied combination fails to disclose all elements of these claims. Thus, considering the lack of disclosure in the applied combination of all elements of claims 1-7, one of ordinary skill in the

art would not find these claims obvious under 35 U.S.C. §103, and therefore the rejections should be overturned.

Independent Claim 1 and Dependent Claims 2-5

Claim 1 recites in part "an operating system ... operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule" (emphasis added). As discussed further hereafter, the applied combination of *Farley* and *Vaidya* fails to teach or suggest at least the above-emphasized element of claim 1. Neither *Farley* nor *Vaidya* discloses a text-file that defines a network-exploit rule and comprises at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule.

The May 15th Office Action alleges that *Farley* discloses the above-emphasized element *see* pages 3-4 of the Office Action. However, *Farley* does not teach a text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system (IPS) evaluates the network-exploit rule.

As discussed further below, *Farley* discloses a database that contains information against which detected events can be compared to, for example, detect relationships between events that is indicative of malicious behavior. Upon occurrence of some activity within the monitored computer system (e.g., receipt of communication packets from a network, etc.), a raw event that contains parameters relating to the activity is generated by an event detection source. The raw events are then communicated to a fusion engine, which can evaluate the events to determine their respective risk, etc., using information from a database. In no instance does *Farley's* system determine from a field of a text-file whether the intrusion protection system is to evaluate a network-exploit rule that is defined in the text file. Indeed, it appears that *Farley's* system

evaluates all raw events against all rules that may be defined in the database (e.g., to determine a respective risk ranking for each raw event and/or a correlation between raw events). While some of the rules defined in the database may not be satisfied by a given raw event, it appears that all received raw events are evaluated against all rules that may be defined in the database. *Farley's* system is discussed in further detail below.

Farley "relates to a method and system for ranking individual security events according to risk and fusing or identifying relationships between two or more security events that may occur on or within a computer system." Paragraph 0003 of *Farley*. *Farley* explains in paragraph 0016:

> The invention can comprise a method and system for managing security information collected from one or more data sources. More specifically, the present invention can comprise a fusion engine which "fuses" or assembles information from multiple data sources and analyzes this information in order to detect relationships between raw events that may indicate malicious behavior and to provide an organized presentation of information to one or more consoles without slowing down the processing performed by the data sources.

Farley explains, in paragraph 0018, that its system may include a database as follows:

> The database may include a raw event classification database that contains categories of different types of raw events. Another database can comprise a context or knowledge database that includes network context information, such as host vulnerability statuses, historical computer event frequency values, and network zone definitions.

Farley also explains, in paragraph 0019, that computer activities on a monitored system may cause events to be detected as follows:

> Real-time raw computer events or raw events may comprise any computer activity that may be tracked by an intrusion detection system as a possible attack on a computer or a plurality of computers. Raw events can be generated by detectors of intrusion detection systems. Each raw event may comprise various parameters that may include, but are not limited to the following: source internet protocol address of the computer activity, destination internet protocol address of

> the computer activity, priority status assigned by the detector, a vulnerability status assigned by the detector, a time stamp, and an event type parameter.

In paragraph 0066, *Farley* explains how the raw events are generated in response to detection of certain computer activities, as follows:

> The detectors 28 of intrusion detection systems scan raw network traffic or local system events for predefined patterns. Once the detectors identify these predefined patterns of information, the detectors generate a raw event which is then sent to the event collector and later to the fusion engine 22.

Figure 5B of *Farley* "illustrates an exemplary raw event 505 that is generated by a detector of an intrusion detection system." Paragraph 0076 of *Farley*. Such raw event 505 includes certain parameters pertaining to a detected computer activity for which such raw event is generated.

Farley proposes a fusion engine that "can determine if one or more real-time raw events are related to each other and if they are part of a larger scheme or computer attack." Paragraph 0020 of *Farley*. "In order to assess risks and determine ranks of real-time raw events, the fusion engine can utilize the aforementioned raw event classification database and the knowledge base." Paragraph 0022 of *Farley*. That is, the "fusion engine can classify raw real-time computer events while also ranking the real-time computer events based upon comparisons with one or more databases." Paragraph 0045 of *Farley*.

In paragraph 0066, *Farley* explains that its fusion engine analyzes the detected raw events as follows:

> The one or more data sources 28 forward their information to the event collector 24. The event collector 24 may comprise one or more program modules designed to store and collect the data received from the one or more data sources 28. The event collector 24 can arrange the data and store it in the event database 26. The event collector 24 also forwards any information received from the data sources 28 to the fusion engine 22. The detectors 28 of intrusion detection systems scan raw network traffic or local system events for predefined patterns. Once the detectors identify these predefined patterns of information, the detectors generate a raw event which is then sent to the event collector and later to the

> fusion engine 22. The fusion engine assembles or fuses the raw events or information received from the event collector 24. In other words, the fusion engine 22 organizes and analyzes the information received from the one or more data sources 28 in order to provide an organized presentation of information by correlating (identifying relationships between) raw computer events that are related to each other.

Farley mentions in paragraphs 0077 and 0089-0090 that raw events may be processed by a CoBRA (Context Based Risk Adjustment) processor that may determine certain CoBRA values for such raw events. In paragraph 0093, *Farley* mentions that the raw computer events may be received from an event collector 24 or an event log file, which might "comprise files having comma separated values (CSV) formats that store computer event data from an intrusion detection system." Thus, the parameters and/or determined CoBRA values for an event that is detected for some computer activity may be stored to a log file in a CSV format.

In view of the above, it should be noted that nothing in *Farley* teaches or suggests a text-file that defines a network-exploit rule, where the text file comprises at least one field that includes information from which a determination is made as to whether an intrusion protection system (IPS) evaluates the network-exploit rule. While *Farley* mentions a database that contains information against which detected events can be compared to, for example, detect relationships between events that is indicative of malicious behavior, *Farley's* system evaluates all raw events against all rules that may be defined in the database (e.g., to determine a respective ranking of risk for each raw event). The database is not taught as comprising a field that includes information from which a determination is made as to whether an intrusion protection system (IPS) evaluates the network-exploit rule defined in the database. Instead, all such rules appear to be evaluated. Indeed, *Farley* explains in paragraph 0064 that "Information from the databases are typically loaded into fusion engine 22 that comprises high memory devices such as random access memory (RAM) since comparisons between raw events and the databases must be performed in a very rapid and in a very efficient manner." Thus, while the database of *Farley* might define rules (e.g., for correlating events and/or determining a risk to be assigned a given event), the database does not include a field that includes information from which a

determination is made as to whether an intrusion protection system (IPS) evaluates the rule defined in the database. Instead, all rules in the database appear to be evaluated in *Farley*.

Additionally, as discussed above, *Farley* mentions that upon occurrence of some activity within the monitored computer system (e.g., receipt of communication packets from a network, etc.), a raw event that contains parameters relating to the activity is generated by an event detection source. The raw events may include information pertaining to the detected activity, which might be formatted in a CSV format. However, such raw events do not define a network-exploit rule. Rather, the raw events merely specify parameters that pertain to a detected activity on a monitored computer (e.g., source internet protocol address of the computer activity, timestamp of the activity, etc.). Additionally, the raw events do not have a field that includes information from which a determination is made as to whether an intrusion protection system (IPS) evaluates a rule that is defined in such raw event (again, no rule is defined in the raw events).

Accordingly, *Farley* fails to teach or suggest at least the above-emphasized element of claim 1. Further, *Vaidya* is not asserted by the Examiner as teaching or suggest this element of claim 1, nor does it do so. Therefore, the combination of *Farley* and *Vaidya* fails to teach or suggest all elements of claim 1, and thus claim 1 is not obvious over this combination of references. Appellant therefore respectfully requests that the rejection of claim 1 be overturned.

Claims 2-5 each depend either directly or indirectly from independent claim 1, and thus inherit all limitations of independent claim 1. It is respectfully submitted that dependent claims 2-5 are allowable at least because of their dependency from independent claim 1 for the reasons discussed above.

Dependent Claim 6

Dependent claim 6 depends from claim 5, which depends from claim 2, which depends from independent claim 1. Thus, claim 6 includes all of the limitations of claims 1, 2, and 5 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 6 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 5 recites "the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network." Claim 6 further recites: "wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value." The combination of *Farley* and *Vaidya* fails to teach or suggest this further element of claim 6.

Neither *Farley* nor *Vaidya* teaches or suggests transmitting a subset of a plurality of machine-readable signature files to another node, wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value. Indeed, neither *Farley* nor *Vaidya* appear to disclose generating machine-readable signature-files from a text-file, and certainly not from a text-file having an asserted ENABLED field value.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 6 be overturned.

Dependent Claim 7

Dependent claim 7 depends from claim 5, which depends from claim 2, which depends from independent claim 1. Thus, claim 7 includes all of the limitations of claims 1, 2, and 5 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 7 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 5 recites "the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network." Claim 7 further recites: "wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold." The combination of *Farley* and *Vaidya* fails to teach or suggest this further element of claim 7.

Neither *Farley* nor *Vaidya* teaches or suggests transmitting a subset of a plurality of machine-readable signature files to another node, wherein the subset comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than a received threshold. Indeed, neither *Farley* nor *Vaidya* appear to disclose generating machine-readable signature-files from a text-file, and certainly not from a text-file having a SEVERITY field value.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 7 be overturned.

B. Rejections under 35 USC §102 over *Farley*

Claims 8-20 are rejected under 35 U.S.C. §102(e) as being anticipated by *Farley*. To anticipate a claim under 35 U.S.C. § 102, a single reference must teach every element of the claim, see M.P.E.P. § 2131. Appellant respectfully submits that claims 8-20 are not anticipated by *Farley* because *Farley* fails to teach each and every element of the claims, as discussed further below.

Independent Claim 8 and Dependent Claims 9-10

Claim 8 recites:

> A method of distributing command and security updates in a network having an intrusion protection system, comprising:
> generating a text-file defining a network-exploit rule; and
> specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.

Farley fails to teach all of these elements of claim 8. For instance, *Farley* does not teach specifying an ENABLED field value or a SEVERITY level field value during generation of a text file that defines a network-exploit rule.

As discussed above with claim 1, *Farley* appears to describe a database that includes rules that can be used for ranking risk or correlating raw events. However, *Farley* provides no teaching of specifying an ENABLED field value or a SEVERITY level field value during generation of such database.

Further, as discussed above with claim 1, *Farley* appears to describe a raw event that is generated upon occurrence of some activity within the monitored computer system. The raw event contains parameters relating to the activity, where such information might be formatted in a CSV format. However, such raw events do not define a network-exploit rule. Rather, the raw events merely specify parameters that pertain to a detected activity on a monitored computer (e.g., source internet protocol address of the computer activity, timestamp of the activity, etc.).

Thus, *Farley* fails to teach specifying an ENABLED field value or a SEVERITY level field value during generation of a text file that defines a network-exploit rule, and therefore claim 8 is not anticipated by *Farley*. Therefore, Appellant respectfully requests that the rejection of claim 8 be overturned.

Claims 9-10 each depends either directly or indirectly from independent claim 8, and thus inherit all limitations of independent claim 8. It is respectfully submitted that dependent claims 9-10 are allowable at least because of their dependency from independent claim 8 for the reasons discussed above.

Dependent Claim 11

Dependent claim 11 depends indirectly from independent claim 8, and thus includes all of the limitations of claim 8 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 11 is allowable at least because of its dependence from claim 8 for the reasons discussed above.

Claim 10 recites "transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network." Claim 11 depends from claim 10 and further recites: "wherein the subset of machine-readable signature-files comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files that has the respective ENABLED field asserted." *Farley* fails to teach this further element of claim 11.

Farley does not teach transmitting a subset of a plurality of machine-readable signature files to another node, wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value. Indeed, *Farley* does not appear to disclose generating machine-readable signature-files from a text-file, and certainly not from a text-file having an asserted ENABLED field value.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 11 be overturned.

Dependent Claim 12

Dependent claim 12 depends indirectly from independent claim 8, and thus includes all of the limitations of claim 8 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 12 is allowable at least because of its dependence from claim 8 for the reasons discussed above.

Claim 10 recites "transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network." Claim 12 depends from claim 10 and further recites: "specifying a priority level threshold, the subset of the plurality of machine-readable signature-files comprised of all machine-readable signature-files generated from a respective one of the plurality of text-files having a SEVERITY level field value equal to or greater than the threshold." *Farley* fails to teach this further element of claim 12.

Farley does not teach transmitting a subset of a plurality of machine-readable signature files to another node, wherein the subset comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than a received threshold. Indeed, *Farley* does not appear to disclose generating machine-readable signature-files from a text-file, and certainly not from a text-file having a SEVERITY field value.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 12 be overturned.

Dependent Claim 19

Dependent claim 19 depends from independent claim 8, and thus includes all of the limitations of claim 8 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 19 is allowable at least because of its dependence from claim 8 for the reasons discussed above.

Additionally, claim 19 further recites "wherein the ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system, and wherein the SEVERITY level field value specifies a severity level of the network-exploit rule." *Farley* fails to teach this further element of claim 19.

As mentioned above with claim 8, *Farley* does not teach specifying an ENABLED field value or a SEVERITY level field value during generation of a text file that defines a network-exploit rule. Further, *Farley* does not teach that an ENABLED field specifies whether the network-exploit rule is enabled for evaluation by an IPS. Further, *Farley* does not teach a SEVERITY level that specifies a severity of a network-exploit rule.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 19 be overturned.

Dependent Claim 20

Dependent claim 20 depends from independent claim 8, and thus includes all of the limitations of claim 8 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 20 is allowable at least because of its dependence from claim 8 for the reasons discussed above.

Additionally, claim 20 further recites:

> distributing the network-exploit rule and the at least one field to a plurality of nodes; and
>
> determining by an intrusion protection system of each of the plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node.

Farley fails to teach this further element of claim 20. *Farley* fails to provide any teaching whatsoever of determining by an intrusion protection system of each of a plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node. As discussed above with claim 1, *Farley* instead appears to evaluate all rules defined in a database, rather than determining based at least in part on one field whether the IPS is to evaluate such rule.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 20 be overturned.

Independent Claim 13 and Dependent Claims 14 and 16

Claim 13 recites in part "compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field." *Farley* fails to teach at least this element of claim 13.

As discussed above with claim 1, *Farley* appears to describe a database that includes rules that can be used for ranking risk or correlating raw events. However, *Farley* provides no teaching of its database comprising a value of an ENABLED field or a SEVERITY field. Further,

Further, as discussed above with claim 1, *Farley* appears to describe a raw event that is generated upon occurrence of some activity within the monitored computer system. The raw event contains parameters relating to the activity, where such information might be formatted in a CSV format. However, such raw events do not comprise machine-readable logic representative of a network-exploit rule. Rather, the raw events merely specify parameters that pertain to a detected activity on a monitored computer (e.g., source internet protocol address of the computer activity, timestamp of the activity, etc.).

Thus, *Farley* fails to teach at least the above-identified element of claim 13, and therefore claim 13 is not anticipated by *Farley*. Therefore, Appellant respectfully requests that the rejection of claim 13 be overturned.

Claims 14 and 16 each depend either directly or indirectly from independent claim 13, and thus inherit all limitations of independent claim 13. It is respectfully submitted that dependent claims 14 and 16 are allowable at least because of their dependency from independent claim 13 for the reasons discussed above.

Dependent Claim 15

Dependent claim 15 depends indirectly from independent claim 13, and thus includes all of the limitations of claim 13 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 15 is allowable at least because of its dependence from claim 13 for the reasons discussed above.

Claim 15 recites "further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold." (Emphasis added). *Farley* fails to teach this further element of claim 15. That is, *Farley* does not teach transmitting a machine-readable signature file to another node upon determining that the value of a SEVERITY field is greater than a received threshold.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 15 be overturned.

Dependent Claim 17

Dependent claim 17 depends indirectly from independent claim 13, and thus includes all of the limitations of claim 13 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 17 is allowable at least because of its dependence from claim 13 for the reasons discussed above.

Claim 17 recites "further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the ENABLED field value is logically asserted." (Emphasis added). *Farley* fails to teach this further element of claim 17. That is, *Farley* does not teach transmitting a machine-readable signature file to another node upon determining that the ENABLED field value is logically asserted.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 17 be overturned.

C. Conclusion

In view of the above, Appellant requests that the board overturn the outstanding rejections of claims 1-20. Attached hereto are a Claims Appendix, Evidence Appendix, and Related Proceedings Appendix. As noted in the attached Evidence Appendix, no evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted. Also, as noted by the Related Proceedings Appendix, no related proceedings are referenced in II above, and thus no copies of decisions in related proceedings are provided.

No fee is believed to be due with this Appeal Brief. If any additional fee is due, please charge Deposit Account No. 08-2025, under order No. 10017334-1 from which the undersigned is authorized to draw.

Respectfully submitted,

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: July 26, 2007

Signature: Donna Forbit
(Donna Forbit)

By _____
Jody C. Bishop
Registration No.: 44,034
Attorney/Agent for Applicant
Dated: July 26, 2007
Telephone (214) 855-8007

VIII – CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 10/003,820:

1. A node of a network for managing an intrusion protection system, the node comprising:

a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule.

2. The node according to claim 1, wherein the at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field.

3. The node according to claim 1, wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the machine-readable signature-file to at least one other node of the network.

4. The node according to claim 1, further comprising a database, the node operable to store a plurality of text-files, each respectively defining a network-exploit rule, in the database.

5. The node according to claim 2, further comprising a machine-readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files, the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network.

6. The node according to claim 5, wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

7. The node according to claim 5, wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold.

8. A method of distributing command and security updates in a network having an intrusion protection system, comprising:

generating a text-file defining a network-exploit rule; and

specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.

9. The method according to claim 8, further comprising storing a plurality of text-files in a database, each text-file defining a network-exploit rule.

10. The method according to claim 9, further comprising transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network.

11. The method according to claim 10, wherein the subset of machine-readable signature-files comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files that has the respective ENABLED field asserted.

12. The method according to claim 10, further comprising specifying a priority level threshold, the subset of the plurality of machine-readable signature-files comprised of all machine-readable signature-files generated from a respective one of the plurality of text-files having a SEVERITY level field value equal to or greater than the threshold.

13. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading input from an input device of the computer;

compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field;

evaluating the machine-readable signature file; and

determining the value of the at least one field of the machine-readable signature file.

14. The computer readable medium according to claim 13, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of specifying a SEVERITY threshold value.

15. The computer readable medium according to claim 14, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold.

16. The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of generating a text-file from the input, the text-file specifying the network-exploit rule and the at least one field, the machine-readable signature file compiled from the text file.

17. The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the ENABLED field value is logically asserted.

18. The node according to claim 1 wherein the intrusion protection system management application is further operable to determine, based at least in part on the at least one field, ones of a plurality of other nodes to which the network-exploit rule is to be distributed.

19. The method according to claim 8 wherein the ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system, and wherein the SEVERITY level field value specifies a severity level of the network-exploit rule.

20. The method according to claim 8 further comprising:

distributing the network-exploit rule and the at least one field to a plurality of nodes; and

determining by an intrusion protection system of each of the plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node.

IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS APPENDIX

No related proceedings are referenced in II above, and thus no copies of decisions in related proceedings are provided.